Universidad Zaragoza
1542

Trabajo Fin de Grado

Configuración segura de radioenlaces IP para la unión de puestos de mando

Autor

Adrián Martínez López

Directores

Dra. Doña María Teresa Sánchez Rúa
Cap. Don Jorge Huertos Aparicio

Centro Universitario de la Defensa-Academia General Militar

Año 2019

Resumen

El sistema actual de transferencia de voz y datos entre los diferentes puestos de mando de una brigada se está quedando obsoleto. Esto ocurre debido a que el sistema actual es analógico y las frecuencias que se emplean caducan próximamente. Además, el ancho de banda máximo del sistema actual es muy inferior al requerido a día de hoy debido a la velocidad con la que evolucionan las nuevas tecnologías. Por ello, surge la necesidad de implantar un sistema de radioenlaces IP que permita un enlace fiable y seguro con el que consiga mantener un constante enlace. Además, esta tecnología IP permite la utilización de distintos sistemas de mando y control que actualmente necesitan de comunicaciones satélite para transferir los datos entre los puestos de mando. Por tanto, este trabajo surge de la necesidad de renovar el sistema de radioenlace terreno actual por uno que ofrezca mejores capacidades.

Sus objetivos son, primeramente, determinar que tipos de transmisores y antenas cumplen con las capacidades necesarias para trabajar en los ambientes en los que opera el Ejército de Tierra. Para esto se necesita de un sistema de radioenlaces IP fiable que permitan mantener un enlace constante entre los PCs.

Una vez realizado este estudio se ha procedido a configurar el sistema de la forma más segura posible. Además, se han tomado las medidas necesarias para lograr un sistema robusto frente a posibles ataques. Una vez conseguido esto, se logra que toda la información pueda transferirse entre los PCs de forma segura.

Las conclusiones a las que se ha llegado pueden ser de utilidad para las distintas brigadas del Ejército de tierra a la hora de adquirir material con el que enlazar sus puestos de mando y la configuración que se ha de realizar para que la información sensible que manejan esté protegida contra personal no autorizado. Se ha tener en cuenta que el sistema propuesto no deja de ser un sistema de uso civil por lo que la implementación de este debe ser utilizada mientras se desarrollan otros sistemas destinados exclusivamente al ámbito militar. Aún así, al haberse incorporado al sistema cifradores IP certificados por la OTAN se puede concluir que la información transferida entre los PCs está a salvo de ser extraída.

Abstract

The current system of voice and data transfer between the different command posts (PC) of a brigade is becoming obsolete. This is due to the fact that the current system is analogical, and the frequencies used expire soon. In addition, the maximum bandwidth of the current system is much lower than that required today due to the speed with which new the new technologies evolve. Therefore, the need to implement a system of IP radio links that allows a reliable and secure link with which to maintain a constant connection arises. In addition, this IP technology allows the use of different command and control systems, currently need satellite communications to transfer data between command posts. Therefore, this work arises from the need to renew the current ground radio link system and its aim is to propose a new system offering better capabilities.

The main objective is to determine what types of transmitters and antennas fulfill the necessary capabilities to work in the environments in which the Army operates. This requires a reliable Ip radio link system to maintain a constant connection between PCs. In this work, a suitable architecture and configuration to define a new radio link system is proposed. In order to verify the applicability of this new system, some computer simulations have been carried out, considering two different distances between PCs. Moreover, the new system is verified to work correctly in a real situation.

Once this study has been carried out, the system has been configured in the safest possible way. In addition, the measures needed to achieve a robust system against possible attacks have been taken. Due to these measures, all the information could be securely transferred between PCs.

The conclusions obtained here may be useful for the different brigades of the Army when acquiring material to link their command posts. Moreover, the presented security configuration guarantees that the sensitive information they handle is protected against unauthorized personnel.. It should be borne in mind that the proposed system is still a civilian system, and therefore the implementation of this system should be used while developing other systems intended exclusively for the military field. Even so, since IP encryption systems certified by NATO have been incorporated into the system, it can be concluded that the information transferred between the PCs is safe from being extracted.

Agradecimientos

Me gustaría reconocer el esfuerzo a todas aquellas personas que de una manera u otra han participado en mi formación.

En primer lugar, agradecer la ayuda recibida por todo el personal de la Compañía de Transmisiones de la Brigada “Aragón” I durante las prácticas externas.

En segundo lugar, quiero destacar la ayuda y seguimiento constante de la profesora Mª Teresa Sánchez Rúa en lo referente a este trabajo.

Por último, me gustaría nombrar a mis padres Joaquín y Eva, a mi hermana Alba y a mi pareja Belén que, además de haberme apoyado en todo momento, me han ayudado en los momentos más difíciles durante estos últimos años.

Índice

Índice de figuras

Lista de Acrónimos

Acrónimo	**Significado**
BMS	Battle Management System
CCN	Centro Criptológico Nacional
CIATRANS	Compañía de Transmisiones
CIS	Sistemas de Información y Telecomunicaciones
COMSEC	Comunicación Segura/ *Communications Security*
CT	Centro de Transmisiones
CTPC	Centro de Transmisiones del Puesto de Mando
dBm	Decibelio-milivatio
F	Frecuencia
FAS	Fuerzas Armadas
JCHAT	JointChat
LAN	Red de Área Local
PC	Puesto de Mando / *Command position*
PCALT	Puesto de Mando Alternativo
PCAV	Puesto de Mando Avanzado
PCMOV	Puesto de Mando Móvil
PCPRAL	Puesto de Mando Principal
PCR	Puesto de Mando Retrasado
PCTAC	Puesto de Mando Táctico
PTP	Punto a Punto
RBA	Red Básica de Área
RRC	Red Radio de Combate
SIMACET	Sistema de Mando y Control del Ejército de Tierra
SSID	Identificador de red / *Service Set Identifier*
TDMA	Acceso múltiple por división de tiempo
v	Velocidad de la onda
VoIP	Voz sobre IP/*Voice over IP*
WAN	Red de Área Metropolitana
WEP	*Wired Equivalent Privacy*

WPA	*WIFI Protected Access*
WPA2	*WIFI Protected Access v2*
λ	Longitud de onda

1. Introducción

Actualmente en el Ejército de Tierra se emplea tanto el enlace satélite como la Red Básica de Área (RBA) para la transferencia de información entre los distintos puestos de mando (PC) de una brigada. El radioenlace a través de la RBA se ha quedado obsoleto ya que es analógico y su ancho de banda es muy limitado para las necesidades actuales (512kbps), además de no permitir el radioenlace vía IP. Además, las frecuencias en las que trabaja deberán abandonarse en diciembre de 2019 ya que caduca su uso. No se puede depender únicamente del enlace satélite, por lo que es necesario implementar otro tipo de radioenlaces y estos deben trabajar sobre IP. Esto permitiría el uso de telefonía IP y de videoconferencias, además de dar servicios de sistemas de información para el mando y control del Ejército de Tierra.

Por ello, en algunas unidades se están empezando a utilizar distintos radioenlaces IP civiles debido a su gran ancho de banda y versatilidad, así como un coste muy reducido. El problema de usar estos radioenlaces civiles que han evolucionado muy rápidamente en los últimos años radica en la falta de conocimientos necesarios en las unidades para la protección de esta información de posibles atacantes.

Por otro lado, la información que se maneja en los PCs es muy sensible, por lo que en este proyecto se buscará asegurarla y que esta fluya de manera permanente entre ellos. Será necesario tanto que el enlace sea fiable y resistente a posibles ataques como que la información que se trasmite esté protegida y sea imposible descifrarla en caso de que esta sea interceptada. Para ello será necesario cifrarla mediante un cifrador certificado NATO SECRET. Los radioenlaces entre los PCs serán punto a punto, permitiendo así una mayor dificultad de interceptación de la información por parte del enemigo.

1.1. Objetivos

El objetivo principal de este trabajo es conseguir transferir todo tipo de información entre los distintos puestos de mando de una Brigada a través de radioenlaces IP punto a punto en un ambiente táctico.

Para ello se seleccionará un transmisor fiable para la realización de un radioenlace. Este debe ser lo más resistente posible a interferencias y a la climatología ambiental, aparte de poder establecer comunicación a varios kilómetros de distancia.

Además, la información transferida por este radioenlace debe poder transmitirse de una forma segura por lo que se configurará el transmisor de la antena para que esto sea así. Por último, y debido a la restrictiva normativa del CCN (Centro Criptológico Nacional), se dotará a este sistema de un cifrador OTAN certificado.

1.2. Metodología

Se ha realizado una recopilación inicial de información acerca de los radioenlaces IP para poder abordar los principales problemas en la transmisión de información entre puestos de mando y aportar posibles soluciones para la estabilidad y securización de los radioenlaces. A continuación, se ha llevado a cabo el análisis y diseño de un sistema de radioenlace para comprobar la viabilidad de dicha propuesta, se han realizado varias simulaciones mediante

distintos programas de software. Para completar el estudio, se ha realizado una práctica de campo utilizando una de las soluciones propuestas. Por último, respecto al tema de la seguridad, se ha llevado a cabo la configuración interna de las antenas, modificando distintos parámetros para hacer estas más robustas frente a posibles ataques e interferencias, así como el empleo de cifradores OTAN certificados y el estudio de una seguridad física de los dispositivos.

2. Puestos de mando

Para empezar, hay que definir el concepto de brigada y de Puesto de Mando, sus características, tipos, así como la unidad que se encarga de los Sistemas de Información y Telecomunicaciones (CIS en inglés) presentes en ellos.

"La brigada es una gran unidad constituida, adiestrada y equipada para ser empleada como tal de acuerdo con la doctrina específica terrestre, constituyendo la menor unidad capaz de aplicar de forma sincronizada las capacidades operativas de las que dispone con la suficiente potencia de combate para alcanzar un objetivo en una operación militar."[1]

Cada brigada, con el fin de facilitar el mando, puede articular uno o varios PCs desde los que gestionar todas las operaciones. Debido a que los PCs son lugares desde los que se controlan todas las operaciones, son objetivos de gran rendimiento y se deben adoptar medidas eficaces con el fin de asegurar su protección, duplicidad y supervivencia. En la figura 1 se puede ver el interior de un PC.

Figura 1: Foto del interior de un PC. (Fuente: Ministerio de Defensa)

Se distinguen seis tipos de PC en los que una brigada puede articularse: Puesto de mando principal (PCPRAL), Puesto de mando avanzado (PCAV), Puesto de mando retrasado (PCR), Puesto de mando alternativo (PCALT), Puesto de mando táctico (PCTAC), Puesto de mando móvil (PCMOV).

2.1. Organización

Por razones de seguridad y funcionalidad, cada PC se agrupará en varias zonas:

- El área herciana, donde estarán todos los elementos radiantes se colocará en una zona alejada al resto de áreas. El motivo de esto es evitar que el enemigo detecte a través de la

radiación que emiten dichos elementos la localización exacta del PC. De este modo, se realiza una decepción electromagnética al enemigo.

- El área de energía es donde se colocan todos los equipos que proporcionan energía eléctrica al PC. Esta zona se encuentra alejada del área herciana para minimizar al máximo las posibles interferencias con los equipos de telecomunicaciones.
- El área de explotación es el lugar donde se llevan a cabo las operaciones y están los medios de mando y CIS no radiantes. Posteriormente, en el apartado de seguridad, se explicará más en detalle las medidas seguridad que se adoptan en estas zonas.
- En el área de servicios estarán situados los medios de vida necesarios para el correcto funcionamiento del PC, como pueden ser zonas de descanso, cocina, aseos, etc.

En la Figura 2 se puede ver un ejemplo de despliegue de un Centro de Transmisiones del Puesto de Mando (CTPC) y donde se situarían las distintas áreas

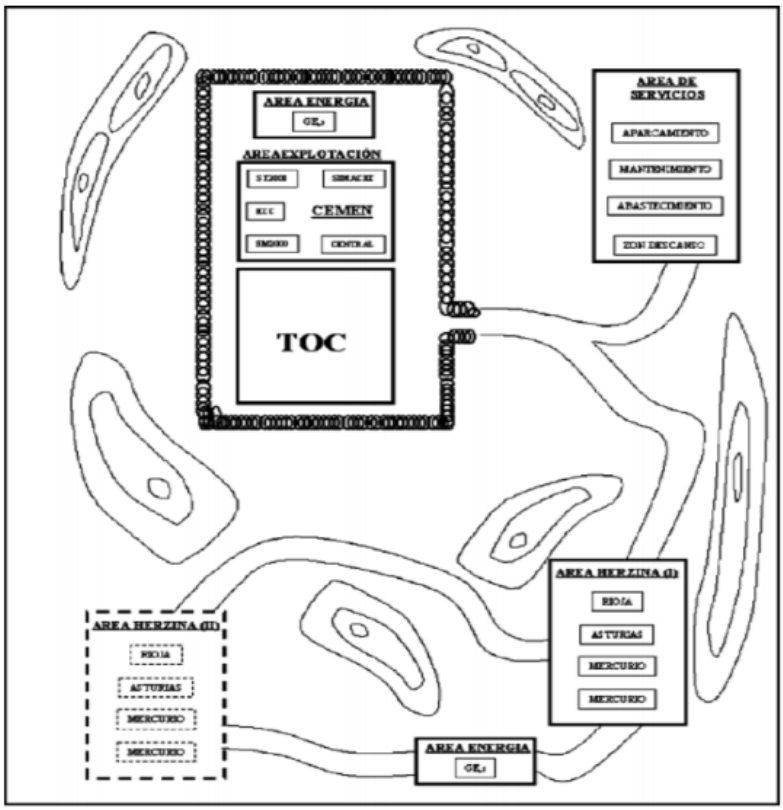


Figura 2: Ejemplo de despliegue del Centro de Transmisiones del Puesto de Mando (CTPC) (Fuente: MADOC)

El propósito de los sistemas CIS es asegurar un enlace constante, no sólo entre los propios PC de la brigada, sino entre estas y las unidades subordinadas. Este tipo de necesidades de enlace se consiguen gracias a las telecomunicaciones.

2.2. Compañía de Transmisiones

Figura 3: Centro de transmisiones de puesto de mando (Fuente: ACING).

La unidad que dota de estos medios a la brigada es la Compañía de Transmisiones (CIATRANS), encuadrada en el batallón de cuartel general de la brigada. Esta unidad se encarga de la puesta en funcionamiento y mantenimiento de los CIS, articulándose en distintos centros de transmisiones (CT) que se superponen a los diferentes PCs de la brigada (Ver Figura 3). La brigada dispone de numerosos medios CIS con los que establecer enlaces como pueden ser la red radio de combate (RRC), la red básica de área (RBA), enlace vía satélite, etc.

2.3. Sistemas de Información

Dentro de los PCs se utilizan una serie de sistemas de información para facilitar el mando y control de las unidades. Estas aplicaciones se transmitirán a través de los radioenlaces IP que se van a estudiar en este proyecto y por ello se detallan a continuación los más importantes:

- SIMACET: Sistema de Mando y Control del Ejército de Tierra. Es la aplicación más importante dentro de un PC, ya que permite un control de las unidades en tiempo real, así como permitir el uso de otros programas como de mensajería o visualización del terreno.
- BMS: Se trata del sistema que permite ejecutar mando y control de pequeñas unidades, es decir, para tipo batallón o grupo, en ambientes tácticos. Dentro de este sistema hay numerosas aplicaciones específicas como pueden ser de apoyo logístico y apoyo al combate.
- TALOS: Es el sistema que usan los grupos de artillería de campaña (GACA) para el mando y control de apoyos de fuegos.
- JCHAT: Esta es una herramienta OTAN que permite el uso de mensajería instantánea en operaciones. Es interoperable entre todas las naciones participantes en la misma misión.

Además de estas aplicaciones, también se transmitirán VoIP (Voice over IP) y videoconferencias.

3. Fundamentos de los radioenlaces IP

3.1. Funcionamiento de los radioenlaces

Se puede definir un radioenlace como la interconexión entre dos puntos de la zona terrestre a través de ondas radioeléctricas, permitiendo la transferencia de información con unas

características de calidad determinadas (Ver Figura 4). El rango de frecuencias mayormente utilizado están comprendidas entre los 800Mhz y los 42Ghz.

El uso de este tipo de radioenlaces en los PCs se realiza como alternativa al cableado o fibra óptica, ya que, en los despliegues, la longitud es demasiado elevada para el uso de estos. Gracias a ellos se consigue el flujo de datos en tiempo real, permitiendo el uso de telefonía IP, videoconferencias, transmisión de datos, etc.

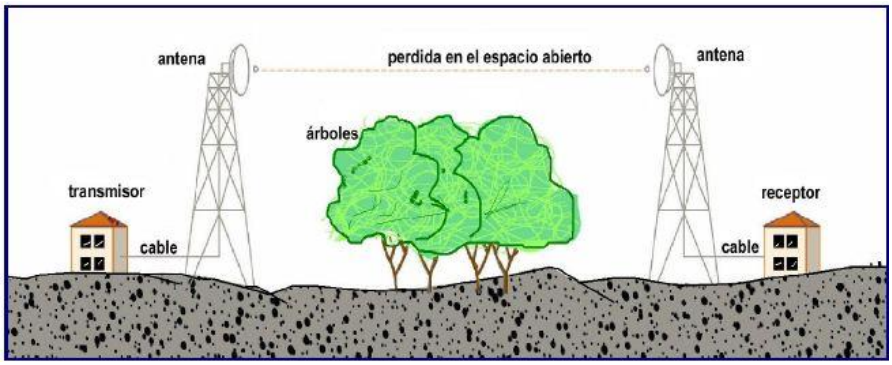


Figura 4: Modelo de radioenlace. (Fuente: www.laleydelboxeo.com)

Para este trabajo, se hará uso de enlaces punto a punto (PTP) con el fin de comunicar exclusivamente dos nodos, concretamente en este caso, dos PCs de brigada.

Las ventajas que presentan respecto de la comunicación por cable son muy numerosas. Entre ellas permiten comunicaciones a gran distancia, abaratar los costes de la infraestructura, así como conseguir una instalación rápida y sencilla.

Por el contrario, existe una serie de desventajas que pueden perjudicar a una correcta comunicación. Entre ellas cabe destacar el problema que pueden causar las condiciones meteorológicas, ocasionando desvanecimientos y problemas en la conexión. Este apartado se tratará en profundidad posteriormente.

3.2. Parámetros de los radioenlaces

En este apartado se estudiarán los distintos parámetros de los radioenlaces y cómo afectan al funcionamiento de estas en los distintos ambientes en los que participan las tropas españolas.[2]

- Ancho de banda: Es la cantidad de datos que se pueden transmitir entre dos puntos de la red por unidad de tiempo. Se mide en bits por segundo.

- Frecuencia: En telecomunicaciones, la frecuencia indica la cantidad de oscilaciones por unidad de tiempo. Una mayor frecuencia permitirá un ancho de banda mayor pero la penetración de las ondas al paso de un obstáculo será peor. Al contrario sucede con una frecuencia baja, donde el ancho de banda será menor pero el alcance mayor. Esto se debe a que la frecuencia está relacionada con la longitud de onda, a través de la relación

$$f = {}^{v}/_{\lambda}$$

donde f denota la frecuencia, v la velocidad de onda y λ la longitud de onda.

- Ancho de canal: El ancho de canal es el espacio que utiliza el enlace en una transmisión radioeléctrica (Ver Figura 5). Un ancho de canal pequeño favorecerá la estabilidad del enlace, pero su capacidad se verá sacrificada, disminuyendo el ancho de banda proporcionado.

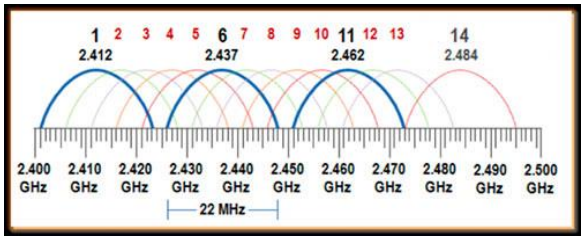


Figura 5: Clasificación de ancho de canal. (Fuente: Wikipedia).

- Polarización: La polarización de una antena es la forma en la que la misma emite la onda electromagnética y se distinguen entre polarización lineal y no lineal. Dentro de la polarización lineal existen dos tipos (Ver Figura 6):

  - Polarización Horizontal: Se dice que la polarización de una onda es horizontal cuando el campo eléctrico de propagación de una onda es paralelo a la tierra.

  - Polarización Vertical: Se dice que la polarización de una onda es vertical cuando el campo eléctrico de propagación de una onda es perpendicular a la tierra.

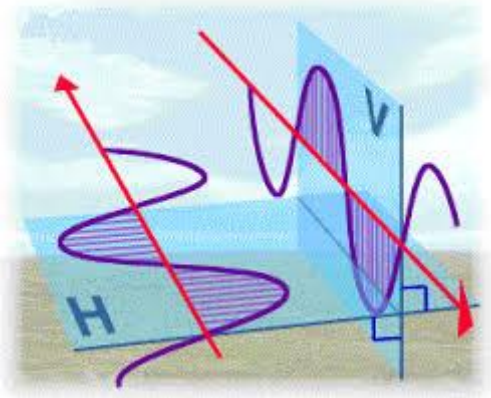


Figura 6: Tipos de polarización lineal. (Fuente: Wikipedia)

- Zona de Fresnel: *"Las zonas de Fresnel son unos elipsoides concéntricos que rodean al rayo directo de un enlace radioeléctrico y que quedan definidos a partir de las posiciones de las antenas transmisora y receptora."*.[3]

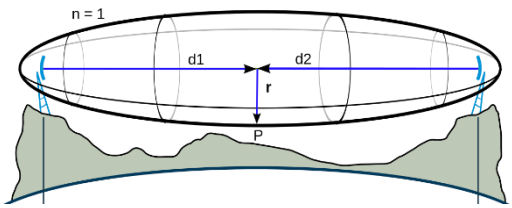


Figura 7: Elipsoide de Fresnel. (Fuente: http://mundotelecomunicaciones1.blogspot.com)

Para que el radioenlace funcione correctamente el primer elipsoide de Fresnel tiene que permanecer, al menos, un 40% del mismo libre de obstrucción (Ver Figura 7).

Para enlaces mayores a 9 kilómetros hay que tener en cuenta la curvatura de la tierra a la hora de realizar los cálculos.

- Ganancia: "*La ganancia de una antena es la relación entre la potencia que entra en una antena y la potencia que sale de esta. Esta ganancia es comúnmente referida en dBi's, y se refiere a la comparación de cuanta energía sale de la antena en cuestión, comparada con la que saldría de una antena isotrópica. Una antena isotrópica es aquella que cuenta con un patrón de radiación esférico perfecto y una ganancia lineal unitaria."* [4]

3.3. Factores externos

En este apartado se mencionan algunos factores externos que han de tenerse en cuenta para la configuración de un radioenlace IP.

- Climatología: El clima puede afectar de manera muy significativa al correcto funcionamiento de los radioenlaces de larga distancia. Los climas áridos y secos son los óptimos mientras que las zonas con hielo y la nieve producen un impacto negativo sobre las antenas debido a la refracción y reflexión.

  Otros fenómenos que pueden afectar a los enlaces son la lluvia y el viento. El primero puede atenuar la señal hasta en un 90% y el segundo afecta a la estructura donde se soporta la antena y a ella misma.

- Línea de Visión Directa (LOS, en inglés): Siempre debe haber LOS entre las antenas del radioenlace para qué este funcione. Además, hay que tener en cuenta que, aunque en los estudios previos del terreno sí exista LOS, puede haber objetos como vegetación o edificios que lo perjudiquen.

- Distancia: Para cada tipo de radioenlace hay una distancia máxima a la que podrán transmitir correctamente. Por ello es importante que esta no se sobrepase y, en caso de que sea mayor, se haga uso de repetidores intermedios.

3.4. Estándares de transmisión de datos

A continuación, se detallarán los estándares IEEE 802.11 (Wifi) y IEEE 802.16 (Wimax), haciendo una comparativa entre ellos y seleccionando el óptimo para las necesidades de enlace entre dos PCs.

3.4.1. IEEE 802.11 (Wifi)

Ventajas de radioenlaces wifi:

- Alta capacidad de transmisión de datos: Debido a las altas frecuencias en las que trabaja la tecnología wifi, el ancho de banda que puede proporcionar es muy alto, incluso a largas distancias.
- Rápida instalación: Necesario en puestos de mando ya que se puede dar el caso en el que se tenga que saltar de posición y las comunicaciones son un objetivo prioritario.
- Costes muy reducidos: Debido a que este estándar esta muy desarrollado e implementado, los costes se reducen considerablemente.
- No requiere grandes conocimientos técnicos: No se requiere de unos conocimientos muy avanzados, por lo que cualquier operador podría instalar dichos radioenlaces sin la necesidad de un curso específico.

Inconvenientes de radioenlaces wifi:

- Distancia: La distancia máxima con radioenlaces wifi suele ser menor de 30km. Aun así, esto podría solucionarse con repetidores intermedios.
- Seguridad: Al ser la tecnología WIFI un estándar libre, hay más información acerca de cómo romper la seguridad de dichos radioenlaces.
- Calidad de servicio: Los protocolos de monitorización de datos son bastante pobres en cuanto a calidad de servicio se refiere. Por ello es necesario implantar otro tipo de protocolo como el TDMA (acceso múltiple por división de tiempo), del que posteriormente se hablará en este trabajo.

La Arquitectura de red del estándar IEEE 802.11 está formada por los siguientes componentes (Ver Figura 8):

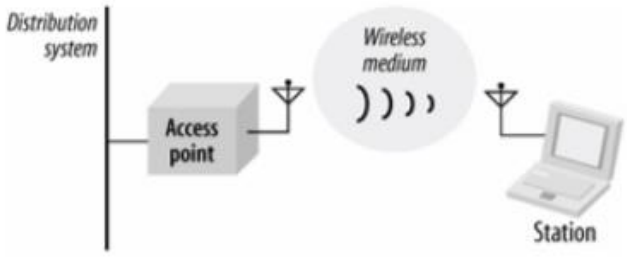


Figura 8: Arquitectura wifi (Fuente: Wikipedia)

- Punto de acceso: Equipo que crea una red de área local inalámbrica (WLAN) a la que se conectan diferentes dispositivos.
- Estación: Dispositivos que se pueden conectar al punto de acceso.
- Medio inalámbrico: Lugar por el que se trasmiten las ondas radioeléctricas.

En el caso de este proyecto, la antena de un PC estará configurada como punto de acceso y la del otro PC como estación. No importa cuál sea cada una ya que simplemente se configurará así para garantizar la conexión entre ambas.

La Figura 9 muestra un esquema de configuración de una red wifi.

Figura 9: Configuración general con dispositivos.

3.4.2. IEEE 802.16 (Wimax)

Ventajas radioenlaces Wimax:

- Permite tener uno ancho de banda mucho más elevado, pudiendo llegar hasta los 300Mbps.

- Trabaja en un rango de frecuencias de rango de 2 a 66 GHz por lo que hay menor riesgo de sufrir interferencias ya que el espectro es mucho más amplio y se puede elegir en cual se quiere trabajar.

- La ventaja más significativa sería la poca latencia que sufren los equipos conectados a través de esta tecnología. La latencia es un valor que indica el tiempo que transcurre desde que se envía la información hasta que llega al destinatario.

Inconvenientes radioenlaces WIMAX:

Antiguamente, la tecnología WIMAX, permitía unos alcances y anchos de banda mucho mayores que los radioenlaces WIFI. Esto ha cambiado durante los últimos años y ahora los enlaces vía WIFI permiten distancias y anchos de banda prácticamente iguales, aunque esta tecnología presente numerosas ventajas, el problema de la necesidad de una certificación y los elevados costes en comparación con el estándar IEEE 802.11 hacen descartar este tipo de tecnología para este proyecto.

La arquitectura de red de WIMAX es análoga a la del WIFI.

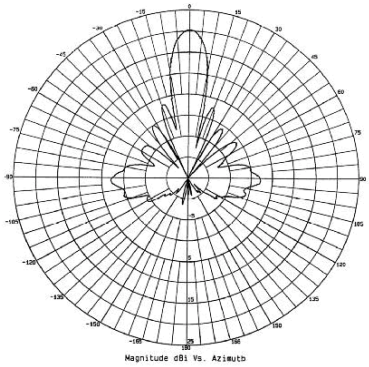
Como **conclusión**, se puede decir que para este proyecto la tecnología WIFI resulta ganadora principalmente por su bajo coste, facilidad de implementación en cualquier ambiente y circunstancia, así como que su frecuencia trabaja en banda libre. Además, en la mayoría de los casos, habría que solicitar el permiso de ciertas frecuencias para el uso WIMAX ya que son frecuencias licenciadas.
Para la unión de dos puestos de mando la latencia no es un factor muy relevante ya que simplemente perjudicaría a las videoconferencias, y, además, prácticamente no habría diferencias entre una latencia de 40ms y otra de 150ms. Con la utilización de la tecnología WIMAX, la latencia sólo depende de la distancia del enlace, mientras que con WIFI también dependería del número de usuarios conectados.

Por último, destacar que el ancho de banda referente a la elección del tipo de estándar no es significativo ya que con un ancho de banda de 10Mbps sería suficiente para cubrir todas las necesidades de transferencia de información.

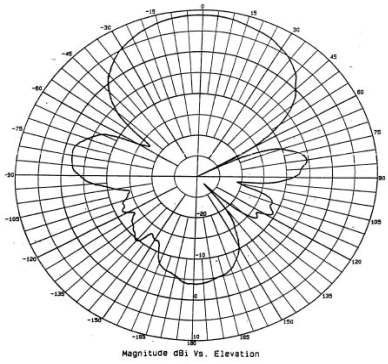
3.5. Tipos de antenas

Una buena elección de antena es vital para poder proporcionar un correcto radioenlace. Dado que el radioenlace a considerar en este trabajo es punto a punto, nos restringimos a antenas con una alta directividad. La directividad de una antena es la relación entre la densidad de potencia que radia la misma en una dirección y la densidad de potencia que radiaría una antena isotrópica a esa misma distancia.

Las antenas más direccionales son las antenas yagui y las antenas parabólicas o parrilla. Como puede apreciarse en la Figura 10, las antenas tipo parabólica concentran casi toda la energía radiada en una misma dirección, mientras que en las Yagui la radiación se dispersa más.
Las primeras suelen ser utilizadas en frecuencias bajas, debido a su pequeño tamaño. Por este motivo no son válidas para nuestro proyecto, ya que las frecuencias en las que trabaja la tecnología WIFI son 2,4GHz y 5 GHz. Por lo tanto, las antenas que a utilizar serán de tipo parabólico gracias a su gran ganancia y direccionalidad. Además, el coste de este tipo de antenas es bastante reducido en comparación con las antenas yagui.



Patrón de Elevación de antena parabólica. (Fuente: WNI)



Patrón de Elevación de antena Yagui. (Fuente: WNI)

Figura 10: Patrones de Elevación

4. Diseño y análisis del sistema

4.1. Necesidades del radioenlace

En este apartado se establecerán las necesidades que ha de cubrir el sistema de radioenlaces IP, según los distintos parámetros explicados en apartados anteriores.

- Ancho de banda: Según personal experto en materia se necesitaría un mínimo de ancho de banda de 10 Mbps para la transmisión de datos entre los dos PCs. Este valor sería suficiente para realizar videoconferencias en paralelo y transmisión de información.

- Ancho de canal: El ancho de canal que utilizan estas antenas está comprendido entre 5 y 40Mhz. Cuanto mayor sea el ancho de canal, existirá mayor capacidad de transmisión, pero la directividad y el alcance será menor. Al contrario, utilizando anchos de canal bajos la energía a la hora de transmitir se concentrará, permitiendo unos alcances mayores, aunque esto será a costa de una reducción del ancho de banda.

  Por ello, como las necesidades de ancho de banda del sistema no superan los 10 Mbps, se intentará que el ancho de canal sea el mínimo posible. Esto dependerá de distintos factores que se tendrían que estudiar para cada tipo de ambiente táctico. Por ejemplo, para radioenlaces donde las distancias sean muy largas, se necesitará concentrar más la energía del radioenlace por lo que se intentará disminuir el ancho de canal. Por otro lado, en radioenlaces donde los PCs estén muy próximos, se podrían utilizar anchos de canal más anchos para tener mayores anchos de banda.

- Frecuencia: Como se ha explicado anteriormente, la frecuencia está relacionada con el alcance de un radioenlace y su capacidad de transmisión. En este caso, para el estándar IEEE 802.11 se puede escoger entre la frecuencia de 2,4Ghz y 5Ghz. En este caso se elegirá la opción de 5Ghz ya que el ancho de banda y la directividad que ofrecen son mucho mayores. Además, como veremos posteriormente en las simulaciones, con la misma antena, trabajando en la banda de 5Ghz se consigue un mejor enlace.

  Por otro lado, cabe destacar que, para frecuencias mayores, el radio necesario de la zona de Fresnel es menor. Por este motivo para los ambientes montañosos en los que las alturas a las que se colocan los radioenlaces tienen que ser más elevadas, será mejor utilizar las frecuencias de 5Ghz antes que las de 2.4Ghz.

  El único motivo por el que se utilizarían las frecuencias de 2.4Ghz sería en caso de lluvias muy intensas ya que al tener una menor frecuencia las interferencias por la lluvia disminuirían.

- Polarización: Para la realización del proyecto resulta más útil que la polarización sea vertical, ya que en caso de que la onda se encuentre con un obstáculo en el terreno, será más fácil que la onda lo supere por encima.

- LOS: Cabe la posibilidad de añadir repetidores en caso de no existir línea de visión directa entre los PCs. Además, si las distancias fueran mayores a las permitidas para cada tipo de radioenlace, se podría colocar un repetidor entre ambos. El repetidor consta de la instalación de dos antenas en un punto intermedio entre los PCs. Una antena recibiría la información de un PC para después, a través de un cable UTP, transferir la información a la antena contigua y finalmente que esta radie los datos al otro PC (Ver Figura 11). También podría utilizarse un switch para conectar las dos antenas del repetidor, aunque esto sólo sería necesario en caso de haber más de 2 antenas.

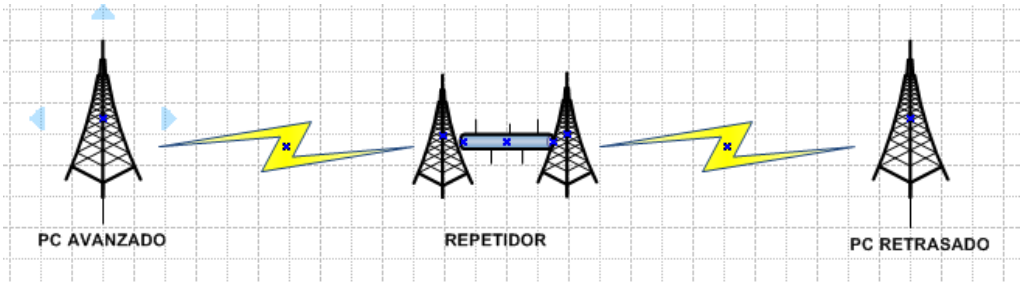


Figura 11: Repetidor colocado entre PCs. (Fuente: Elaboración propia)

- Climatología: Como se ha explicado anteriormente, lo que más puede afectar al correcto funcionamiento del enlace es la lluvia[5], y el viento. Este último puede desviar la dirección de apuntado de la antena y perder el enlace. Por ello la antena que se usará en este trabajo ha de ser ligera y, sobre todo, resistente al viento. El Valle del Ebro, lugar donde se realizarán las pruebas, es una zona muy ventosa, pudiéndose alcanzar rachas de viento de 80km/h. Debido a esto, se escogerá una **antena de rejilla**, que permitirá que el viento le afecte lo menos posible.

- Distancia: La distancia a la que se encuentran dos PCs puede variar entre 5, 30 o incluso 40km. Esto no supondría ningún problema ya que se podrían colocar repetidores intermedios en caso de que las distancias sean muy elevadas o no haya LOS entre ellos.

4.2. Elección de equipos

Considerando todos los parámetros anteriores, se ha llegado a la conclusión de que las antenas Ubiquiti AG-HP-5G27 que posee la Brigada "Aragón" I serían válidas para establecer el radioenlace IP entre los PCs de manera satisfactoria. Además, las antenas Ubiquiti Rocket M5 son las que actualmente se están usando en misiones internacionales. Por ello, se va a proceder a realizar el estudio con dichas antenas.

4.3.Radioenlace Ubiquiti

El sistema de radioenlace propuesto consistirá en las estaciones Ubiquiti Rocket M5 acopladas a una antena parabólica.

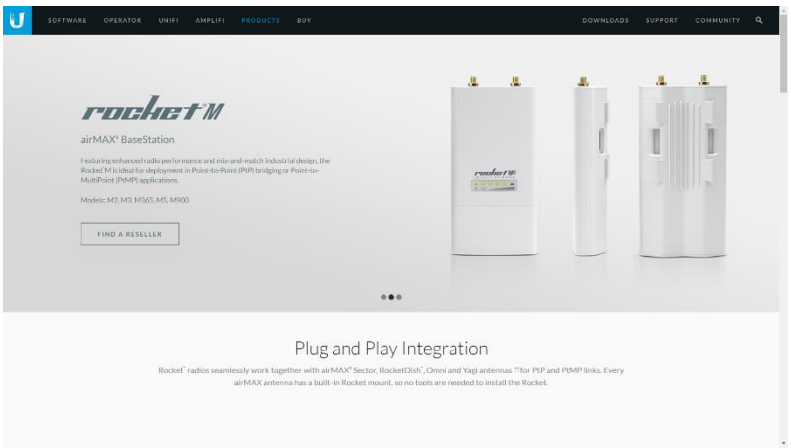


Figura 12: Transmisor Ubiquiti Rocket M5. (Fuente: www.ubnt.com)

Las características técnicas del transmisor se recogen en el ANEXO A

A este transmisor hay que añadirle la antena direccional RocketDish.

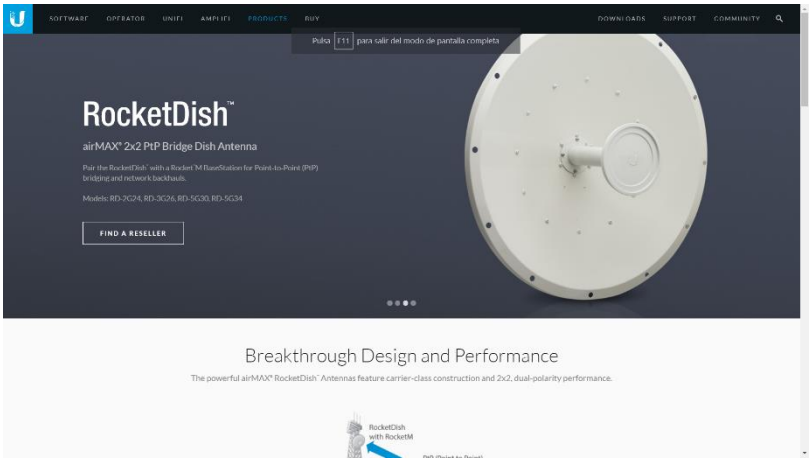


Figura 13: Antena RocketDish 34 dBi. (Fuente: www.ubnt.com)

Ca Las características técnicas de la antena se recogen ANEXO B

Debido a que la unidad no dispone de dichas antenas, pero sí el modelo Ubiquiti AG-HP-5G27 se realizarán las pruebas teóricas con ambas antenas, y si esta última fuera óptima, se realizarán las pruebas reales en el campo de maniobras.

Figura 14: Ubiquiti AG-HP-5G27.
(Fuente: www.ubnt.com)

Las características técnicas de la antena se recogen ANEXO C

4.4. Simulaciones de los radioenlaces

Antes de realizar cualquier radioenlace en el campo de maniobras, es necesario un estudio previo para verificar que habrá enlace entre los Puestos de Mando. Para ello, se van a realizar dos pruebas distintas para comprobar que realmente se puede establecer un intercambio de información entre los dos PCs.

Debido a que los PCs pueden estar situados a varios km, la primera prueba consistirá en un radioenlace a medio alcance (5km) y la segunda de largo alcance (30km).

Dichas simulaciones se llevarán a cabo con el programa de software libre “Radio Mobile”[6] y el

simulador oficial de la empresa Ubiquiti[7]. Las simulaciones con la antena Ubiquiti AG-HP-5G27 sólo se podrán realizar con "Radio Mobile" debido a que este modelo no aparece en el simulador oficial de Ubiquiti.

4.4.1. Consideraciones previas

Hay que tener en cuenta que en las simulaciones el alineamiento de las antenas se considera perfecto. En la práctica esto no suele ser así ya que las antenas se alinean manualmente y las unidades no disponen de GPS con márgenes de error milimétricos.

También hay que destacar la relativa fiabilidad de las simulaciones hechas con la aplicación propia de la marca Ubiquiti.

Por último, para conocer la calidad que tiene un radioenlace hay que fijarse en el "Rx level" o "Nivel de señal". En la siguiente tabla se muestra los valores del nivel de señal (x[1]) asociados a la calidad del enlace.

Nivel de señal	Calidad
-120 dBm < x < -95 dBm	Nula
-95 dBm < x < -83 dBm	Pobre
-83 dBm < x < -71 dBm	Media
-70 dBm < x	Excelente

Tabla 1: Calidad del radioenlace

4.4.2. Simulación de largo alcance

En este caso, hemos seleccionado las dos posiciones de cada PC dentro del campo de maniobras de San Gregorio.

- **PC Avanzado**

Está situado al norte del campo de maniobras San Gregorio, en concreto en el Vértice Esteban[2].

Figura 15: Situación PC Avanzado. (Fuente: Elaboración propia)

[1] Siendo x el nivel de señal obtenido.

[2] Coordenadas Vértice Esteban: 41°56'03.6"N 0°57'01.7"W

- **PC Retrasado**

Está situado en la Academia General Militar (AGM)[3], en concreto en la zona de depósitos.

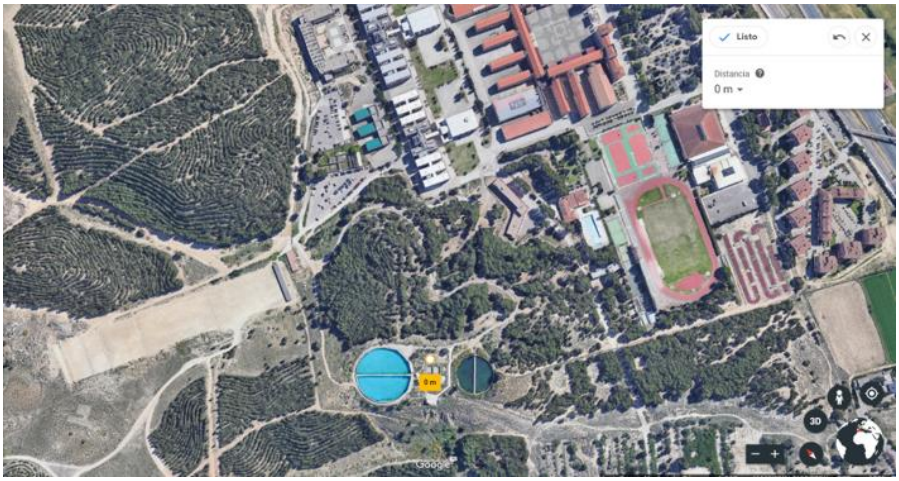


Figura 16: Situación PC Retrasado. (Fuente: Elaboración Propia)

- **Perfil entre los PCs:**

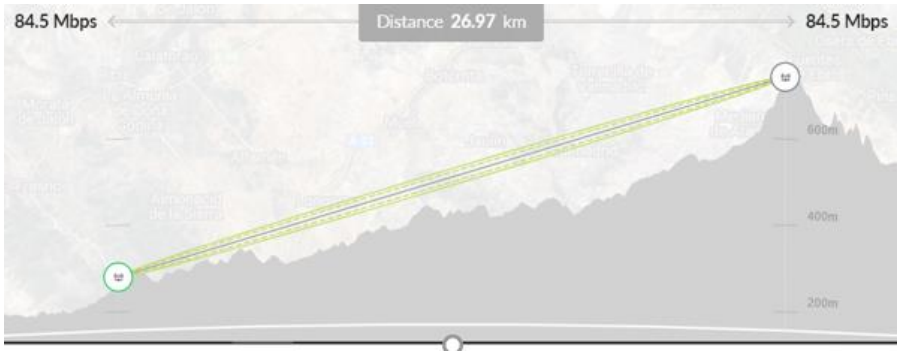


Figura 17: Perfil entre los dos PCs. (Fuente: Elaboración propia)

Como se puede observar, hay una distancia de 26,97km entre los dos PCs, y línea de visión directa. También puede apreciarse que los primeros elipsoides de Fresnel están libres de obstáculos, por lo que en un principio el enlace debería ser satisfactorio.

[3] Coordenadas AGM: 41°41'51.5"N 0°52'37.6"W

❖ **Simulación antena Ubiquiti AG-HP-5G27**

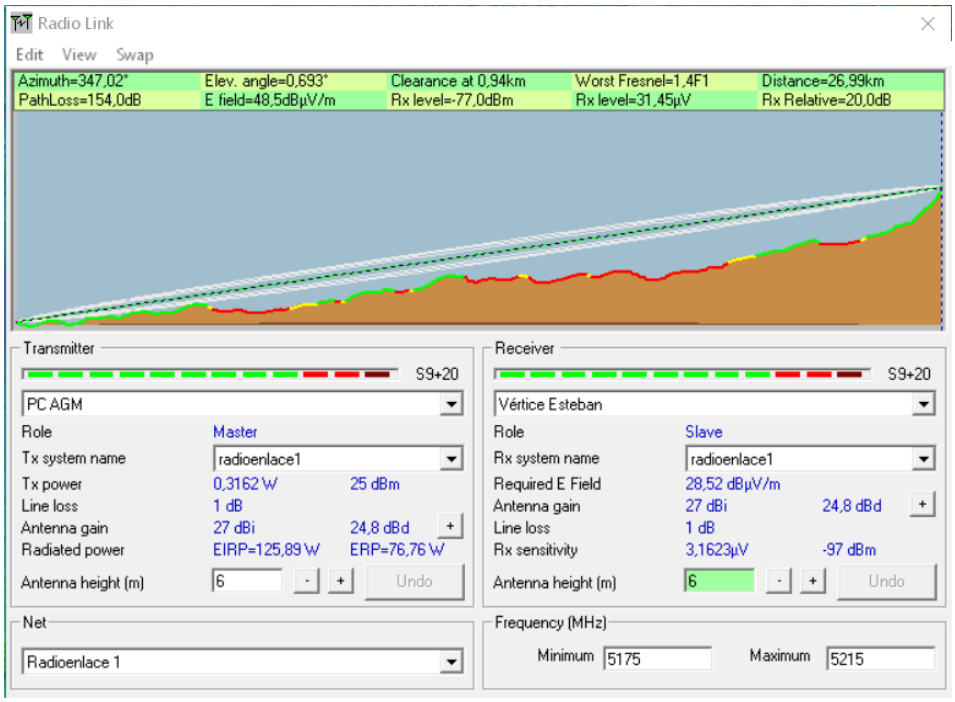


Figura 18: Resultados de la prueba de corto alcance con antena Ubiquiti AG-HP-5G27 (Fuente: Elaboración propia)

Para la simulación de esta antena, se ha utilizado el programa Radio Mobile. Primero se han colocado las coordenadas de los PCs para posteriormente, configurar el radioenlace con los parámetros técnicos de la antena. Como puede observarse en la Figura 18, el radioenlace aparece en color verde y su Rx level es -77dBm. Esto implica que se puede establecer enlace entre los PCs, pero este podría sufrir problemas de conexión con una climatología muy adversa, es decir, fuertes tormentas acompañado de lluvia y viento.

❖ **Simulación antena Rocket M5**

Se ha realizado la simulación con el programa Radio Mobile y como puede apreciarse en la Figura 19, el radioenlace se podrá establecer ya el nivel de señal es de -61 dBm.

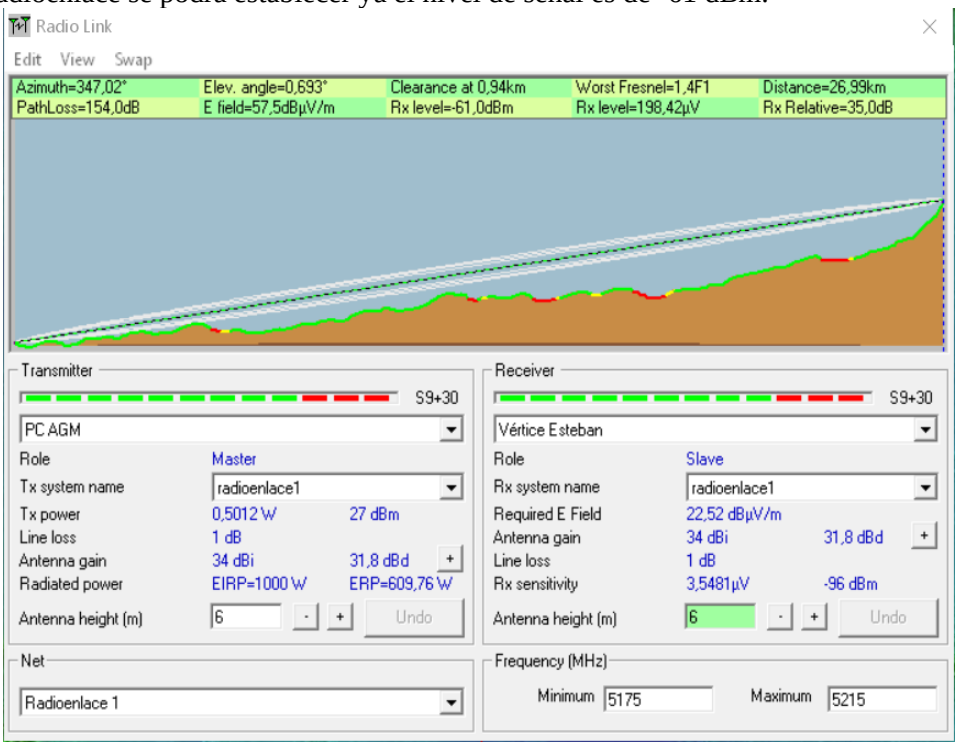


Figura 19: Resultados de la prueba de corto alcance con antena Ubiquiti Rocket M5. (Fuente: Elaboración propia)

4.4.3. Simulación de medio alcance

Para la simulación de medio alcance hemos colocado los dos PC en estas posiciones dentro del campo de maniobras San Gregorio.

❖ **PC Principal**

El PC Principal está situado en la Brigada “Aragón” I[4].

[4] Coordenadas PC Principal: 41°42'59.4"N 0°51'34.3"W

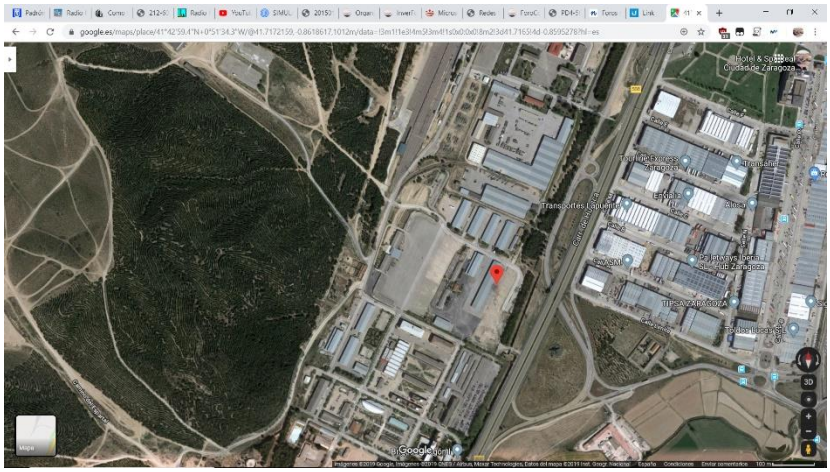


Figura 20: Situación PC Principal. (Fuente: Elaboración propia)

❖ PC Táctico

El PC Táctico está situado al Este de la zona de tiro F23.[5]

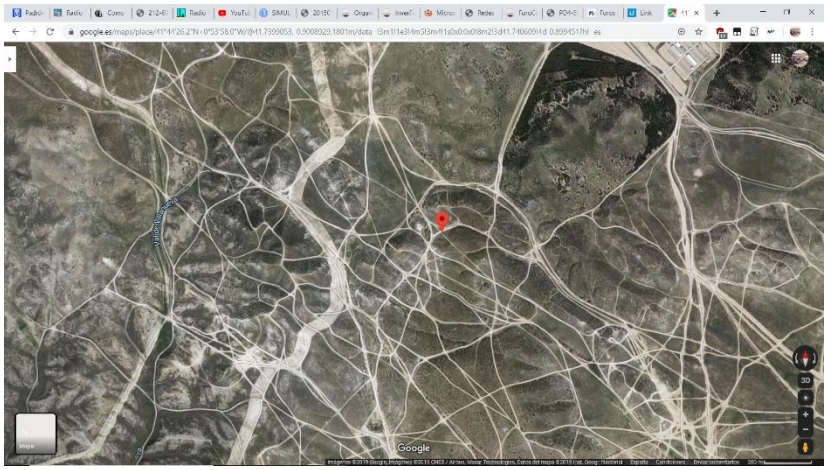


Figura 21: Situación PC Táctico. (Fuente: Elaboración Propia)

❖ Perfil entre los PCs:

Figura 22: Perfil del radioenlace. (Fuente: Elaboración Propia)

[5] Coordenadas PC Táctico: 41°44'26.2"N 0°53'58.0"W

❖ **Simulación antena Ubiquiti AG-HP-5G27**

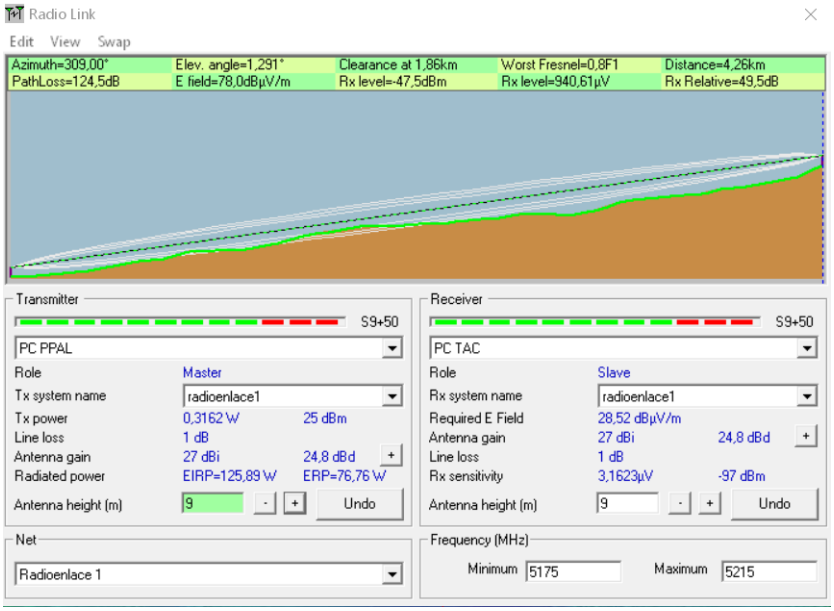


Figura 23: Resultados de la prueba de largo alcance con antena Ubiquiti AG-HP-5G27 (Fuente: Elaboración propia)

Se ha obtenido un nivel de señal de -47,5 dBm por lo que la calidad de señal es excelente.

❖ **Simulación antena Ubiquiti Rocket M5**

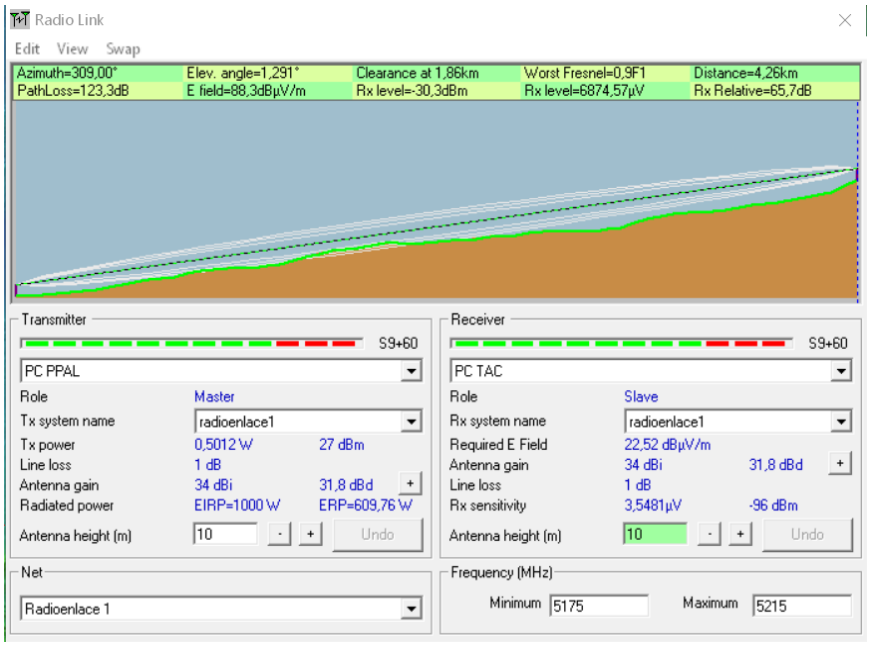


Figura 24: Resultados de la prueba de largo alcance con antena Ubiquiti Rocket M5 (Fuente: Elaboración propia)

Se ha obtenido un nivel de señal de -30,3 dBm por lo que la calidad de señal es excelente, mejorando incluso los resultados obtenidos con la antena anterior.

Las pruebas realizadas con la aplicación de Ubiquiti presentan los mismos resultados que se recogen en el ANEXO D.

Conclusiones de las simulaciones

Como puede apreciarse en ambas simulaciones, los radioenlaces más óptimos se consiguen con la antena Ubiquiti Rocket M5. Aun así, los resultados del radioenlace utilizando la Ubiquiti AG-HP-5G27 son más que fiables. Por ello y debido a que la unidad Brigada "Aragón" I posee dichas antenas, se van a realizar una serie de pruebas en el campo de maniobras con dicha antena para cerciorar su correcto funcionamiento. La prueba se realizará con las posiciones de la simulación de medio alcance.

4.5.Prueba de campo

Para esta prueba de campo, se colocaron dos estaciones con sus respectivas antenas Ubiquiti AG-HP-5G27 en los PC PPAL Y PC TAC de la última simulación. Una vez establecidos en posición y con las antenas alineadas se procedió a realizar una prueba de ping para comprobar que las antenas enlazaban entre sí. Posteriormente, una vez establecido el enlace se realizaron una serie de pruebas que se detallan a continuación.

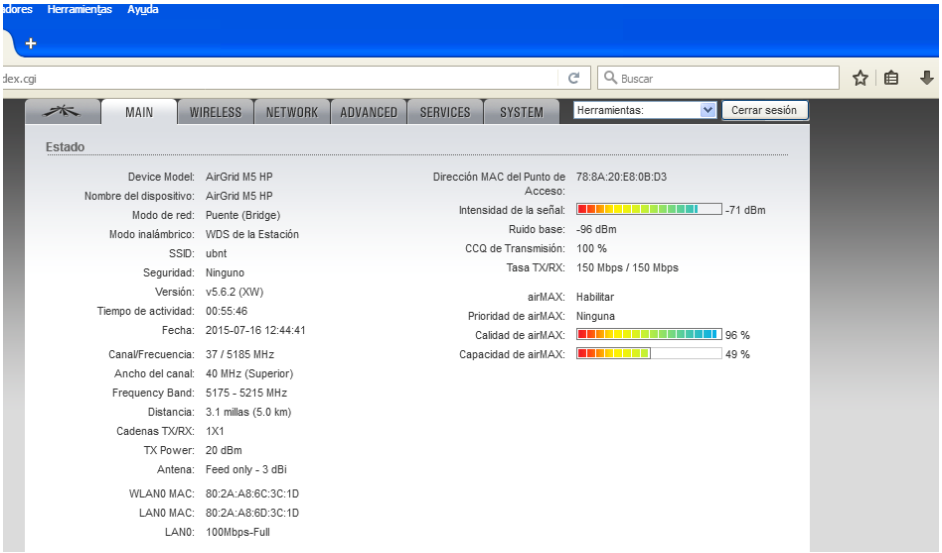


Figura 25:Captura de pantalla de la página de inicio de configuración de la antena. (Fuente: Elaboración propia)

En la Figura 25 se muestra la configuración básica de la antena. Se observa en este caso que la intensidad de señal es de -71dBm, valor que indica que el radioenlace es estable.

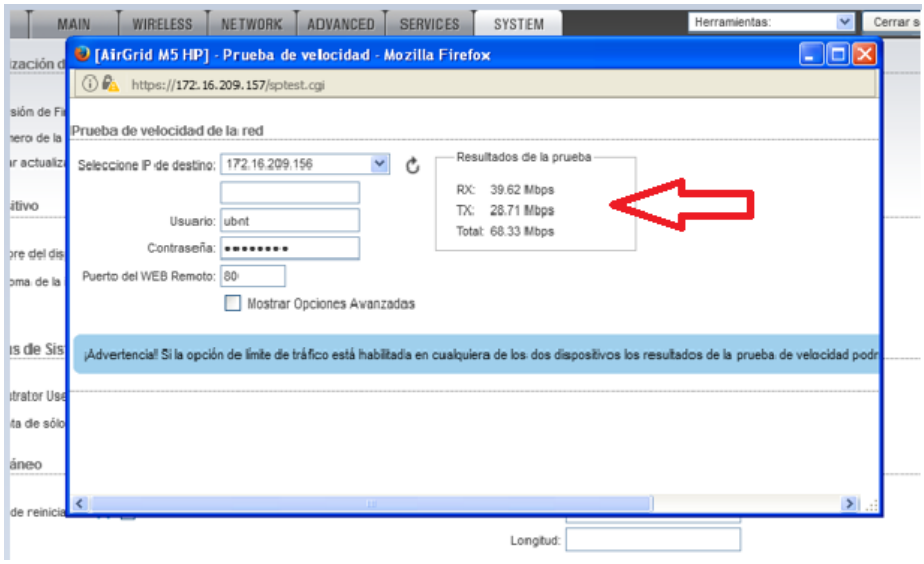


Figura 26:Captura de pantalla de la prueba de velocidad. (Fuente: Elaboración Propia)

Además, se realizó una prueba de velocidad para determinar el ancho de banda disponible. Como se puede comprobar en la Figura 26, se obtuvo un resultado de 68,33 Mbps, resultado muy superior al mínimo establecido para el sistema.

5. Seguridad de los radioenlaces

Todas las brigadas del Ejército son conocedoras de la importancia de la seguridad en la transferencia de datos entre sus puestos de mando, ya que en estos se maneja información sensible que debe acabar en manos no adecuadas. En este trabajo, se propone el uso de radioenlaces IP vía wifi, redes inalámbricas menos seguras que las cableadas.

Una red cableada se asegura prácticamente controlando sus extremos (acceso físico), mientras que, en una red inalámbrica, los datos pueden ser interceptados a mitad de su recorrido ya que las distancias pueden ser muy extensas y no se puede controlar todo ese espacio mediante la presencia de tropas propias.

Todos los datos que se transfieren en un PC están clasificados según el grado de protección de la información que tengan. Los grados de protección son, de mayor a menor: Secreto, reservado, confidencial, difusión limitada y sin clasificar. En el ANEXO E se recoge una breve descripción de cada uno de ellos.

La información con grado de protección Secreto no se puede manejar dentro de un PC según normativa[8] del Centro Criptológico Nacional por lo que no se tratará en este trabajo.

Exponiendo algunos ejemplos, SIMACET tiene carácter reservado y BMS pertenece al grado de difusión limitada, mientras que la telefonía IP tendrá diferentes grados de información dependiendo a que célula esté asociado el teléfono (La información que maneja la célula de operaciones es más sensible que la que se puede manejar en el teléfono del personal encargado de la alimentación).

Para este proyecto, se ha decidido catalogar toda la información como si tuviera carácter reservado y así poder simplificar y economizar toda la arquitectura de red. Según normativa CCN-

STIC 301[8], esto se puede realizar siempre y cuando el grado de seguridad sea el del más elevado. En este caso, reservado.

Los posibles atacantes se sirven de las vulnerabilidades del software o del hardware para lanzar sus ataques, pudiendo realizar suplantación de identidad, manipulación de datos, robos de información o incluso causar una interrupción del servicio.

A continuación, se expone una descripción de lo que es la seguridad de las comunicaciones:

"La Seguridad de las comunicaciones, también conocida por las siglas COMSEC (del inglés Communications Security), es la disciplina que se encarga de prevenir que alguna entidad no autorizada que intercepte la comunicación pueda acceder de forma inteligible a información. Por tanto, esta disciplina incluye campos de estudios como la criptología, la emisión segura, la transmisión segura, la seguridad del flujo del tráfico y la seguridad física del equipo que se encarga de las comunicaciones."[9]

A partir de esta definición y los tipos de amenazas anteriormente escritas, en este proyecto se va a estudiar el tema de la seguridad en 3 bloques diferenciados:

- Emisión y transmisión segura
- Cifrador hardware
- Seguridad física de los equipos

5.1.Emisión y transmisión segura

En este apartado, se tratará la configuración interna de las antenas Ubiquiti para elevar al máximo el nivel de seguridad del radioenlace WIFI. Hay que remarcar que estas antenas funcionan como rúters y por lo tanto pueden configurarse como tal.

Toda la información que se radia por las antenas llega a estas por medio de cableado. Debido a esto, sólo existe riesgo de que la información sea interceptada a través del radioenlace wifi entre los PCs.

Se procederá a configurar los parámetros necesarios para obtener un radioenlace wifi lo más seguro posible. Estas prácticas están recogidas en el siguiente documento oficial del CCN "Guía de Seguridad de las TIC Seguridad en Redes Inalámbricas" [10]

❖ **Menú de acceso**

Para acceder al menú interno "AirOS" de la antena hay que poner la dirección IP de esta en un ordenador. La pantalla que aparecerá será la siguiente:

Figura 27: Menú de inicio de configuración. (Fuente: Elaboración propia)

Para entrar al menú habrá que acceder mediante el usuario y contraseña. Por defecto en este tipo de antenas, el usuario predeterminado es Ubnt y la contraseña 1234.

La primera medida de seguridad será cambiar estas credenciales de acceso por otras más complejas ya que si un intruso consigue entrar dentro de los parámetros de configuración podría cambiar la toda la configuración del radioenlace a su antojo.

Por un lado, se va a cambiar el usuario a "AntenaTFG". Por el otro, para la contraseña, se requiere una longitud mínima de 8 letras, números y caracteres especiales. Además, a ser posible, esta debe ser una palabra que no sea de diccionario, es decir, que no sea una palabra con significado propio, para que sea muy difícil obtenerla mediante fuerza bruta. La contraseña se cambiará a "Pa$$W0rd19".

- **SSID**

Una vez dentro del menú de configuración, se procede a cambiar el nombre de la SSID (Service Set Identifier). El SSID es el nombre con el que se identifica la red del radioenlace. Está definido por defecto y puede mostrar información acerca del radioenlace y sus posibles vulnerabilidades.

Como el radioenlace es punto a punto y solamente se va a conectar entre dos puestos de mando, la opción más segura es ocultar el SSID para que directamente no aparezca (Ver Figura 28).

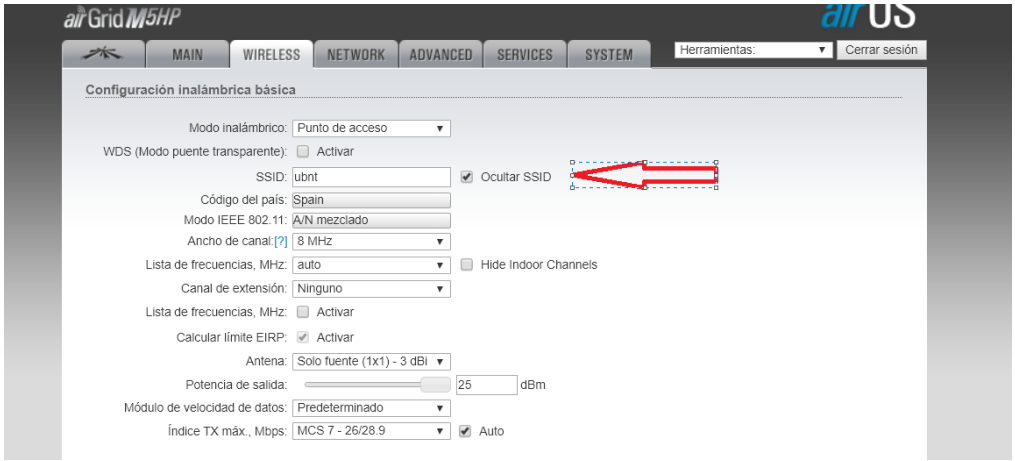


Figura 28: Configuración inalámbrica (Fuente: Elaboración propia)

Se trata de una medida disuasoria, ya que no impide que un posible atacante pueda descubrir el SSID mediante un escaneo de red.

❖ Sistema de cifrado y autenticación

Un aspecto totalmente necesario a la hora de transmitir datos a través de una red es el cifrado de los datos. Existen 3 protocolos posibles para la protección inalámbrica de redes:

- WEP (Wired Equivalent Privacy): Se trata del primer estándar de seguridad wifi que fue implementado en 1999. Actualmente hay demasiadas vulnerabilidades en este protocolo y es muy fácil de romper.

- WPA: (Wifi Protected Access): Este protocolo se adoptó debido a las carencias del WEP. Se basa en la utilización de una clave precompartida (PSK). Aun así, también resultó muy vulnerable a técnicas de intrusión.

- WPA2-AES (Wifi Protected Access, versión 2): La mejora más significativa de este protocolo respecto al WPA fue el uso del AES (Advanced Encryption Standard). Esta mejora fue aprobada por el gobierno estadounidense como método de encriptación válido para información clasificada como de alto secreto.

El protocolo más seguro actualmente es WPA2. Además, según normativa del CNN[8], WPA/WPA2-AES es el método de cifrado óptimo para este tipo de radioenlaces wifi. Por ello en el apartado de seguridad inalámbrica se elegirá este protocolo y la contraseña se modificará como se ha expuesto anteriormente: Longitud mínima de 8 letras y números con caracteres extraños. Además, está se irá cambiando de forma periódica y no será una palabra de diccionario para evitar ataques por fuerza bruta. El tipo de autenticación será basado en claves pre-compartidas (PSK) y en este caso se ha cambiado la contraseña a "Pr0y€ctoTFG2019" (Ver Figura 29).

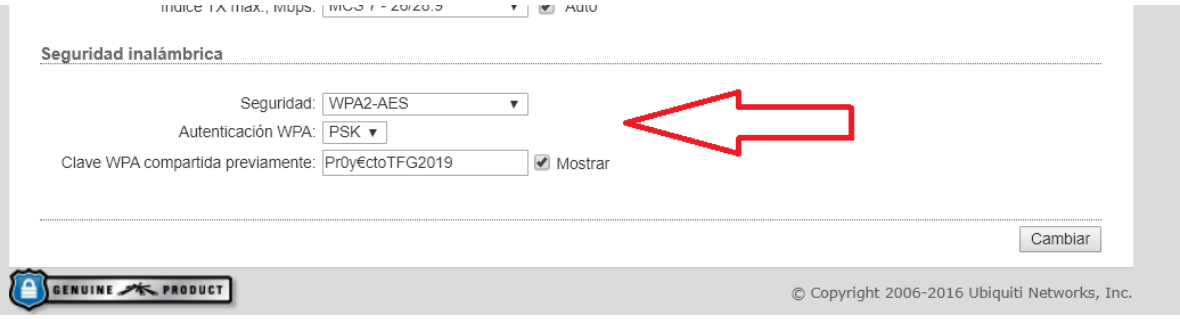


Figura 29: Sistema de cifrado en el radioenlace (Fuente: Elaboración propia)

❖ Filtrado MAC

Otra medida de seguridad que resulta muy útil es el filtrado MAC. Este método consiste en seleccionar las direcciones MAC, también llamadas direcciones físicas, que se pueden conectar a la red y así crear una lista de los dispositivos que pueden conectarse al radioenlace. Estas direcciones son únicas para cada tarjeta de red y la diferencian del resto. Están formadas por 48 bits y 6 grupos de números expresados en hexadecimal. Un ejemplo de dirección MAC sería: 82:38:1A:42:CA:8F.

Esta medida tiene dos inconvenientes. El primero es que es necesario conocer de antemano todos los dispositivos que se van a conectar al radioenlace para seleccionar su MAC. Además, cabe la posibilidad de tener que cambiar esta lista a mitad de la maniobra si se necesitasen añadir nuevos dispositivos. El segundo problema es que este método de seguridad no es infalible ya que hay formas de simular la MAC de otro dispositivo que no es el propio y así poder acceder a la red.

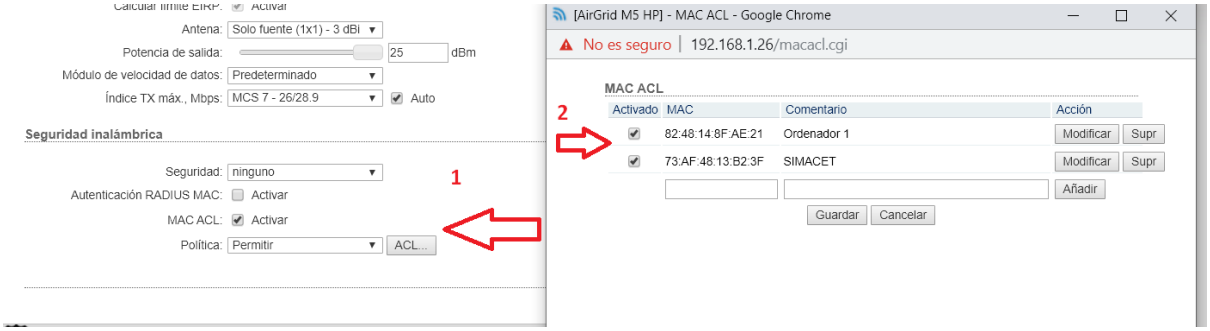


Figura 30: Listado de filtrado MAC (Fuente: Elaboración propia)

Como puede observarse en la Figura 30. Primero hay que activar la lista MAC ACL y el segundo paso consiste en añadir los dispositivos con sus direcciones MAC a la lista.

- **Frecuencias empleadas**

Otro aspecto importante para la fiabilidad del radioenlace es la elección correcta de las frecuencias en las que este va a trabajar. Primero se debe hacer un escaneo de las frecuencias para detectar qué canales hay libres por si surgen problemas de interferencias.

En la prueba de campo descrita en el apartado 3.10, se realizó un escaneo de las frecuencias. Dicho escaneo se recoge en la Figura 31.

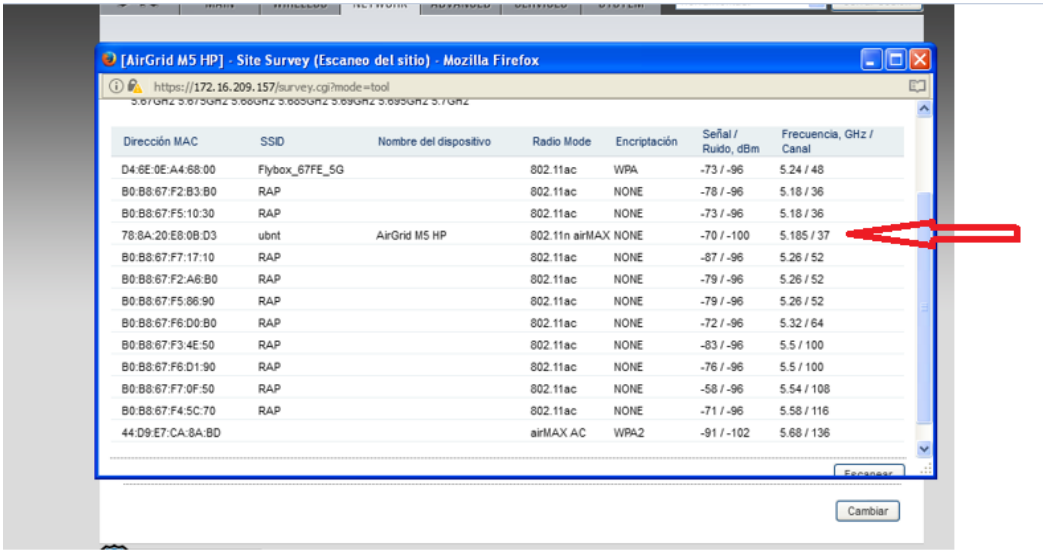


Figura 31: Prueba de escaneo de frecuencias (Fuente: Elaboración propia)

Una vez realizada la prueba se escogió la frecuencia de 5.185GHz y el canal 37 por estar libre. Esta medida ha de realizarse periódicamente y tratar siempre de escoger un canal libre.

- **Limitación de rango de direcciones IP**

En la red WAN de los radioenlaces siempre estarán conectadas las dos antenas, por lo que podemos limitar el rango de direcciones IP a 4: las dos propias de cada antena, la dirección de red y la dirección broadcast. La dirección de red es la que identifica la red utilizada y la dirección broadcast es la que utiliza para permitir la comunicación de todos los dispositivos a esa red.

Esto haría la red mucho más segura ya que impediría conectarse a cualquier otro dispositivo.

Para realizar esto habría que poner la máscara de red como /30, es decir 255.255.255.252. Esto se realiza de esta forma ya que tendríamos libre 4 direcciones.

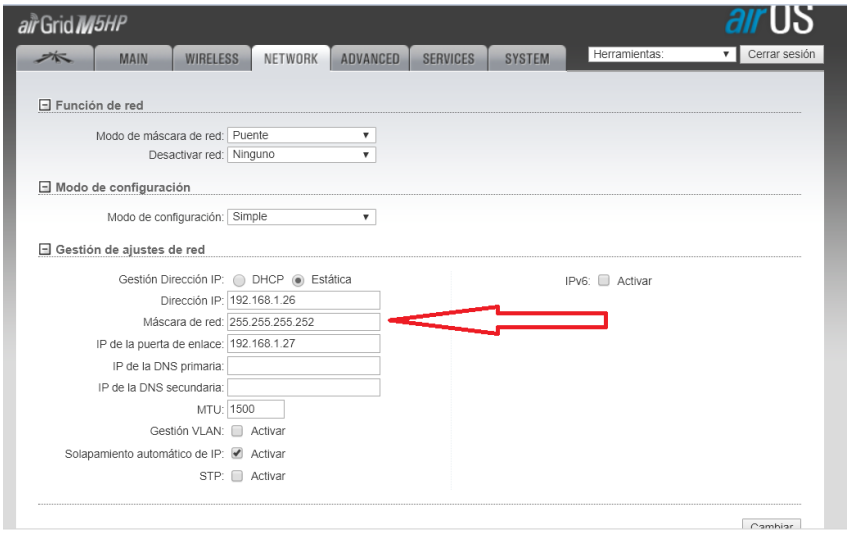


Figura 32: Configuración de la máscara de red (Fuente: Elaboración propia)

❖ Cambio de puertos predeterminados

Cambiar los puertos que vienen predeterminados protegerá en cierta medida el radioenlace de posibles ataques automatizados a puertos conocidos (Ver Figura 33). Aun así, esta medida en sí misma no protege de un intruso que intente atacar directamente contra la red del radioenlace.

Figura 33: Puertos de configuración (Fuente: Elaboración propia)

Por último, es importante tener el servidor telnet desactivado. Este servidor permite un acceso remoto desde otro dispositivo. Por ello como medida extra de seguridad es conveniente que esté desactivado.

5.2. Cifrador hardware

En este apartado se explicará en qué consiste el cifrado de archivos y quien es el organismo que lo regula este proceso en las Fuerzas Armadas (FAS).

El cifrado consiste en alterar la información mediante uno o varios algoritmos matemáticos para transformar un dato legible en otro ilegible. Al destinatario, para descifrarlo, le haría falta la clave

con la que fue encriptado. Es por ello que, si un intruso llegara a interceptar un mensaje a través del radioenlace wifi, no podría acceder a la información que este contiene por no disponer de la clave.

El organismo que regula el uso de la criptología en las FAS es el Centro Criptológico Nacional (CCN).

Para este trabajo, la forma más segura de proteger los datos es empleando el método de extremo a extremo, es decir, mantener las conexiones cifradas entre el equipo de donde sale la información y el que la recibe. Por ello se utilizarán cifradores IP tipo hardware. En concreto, el Cifrador IP táctico EP430T. Este cifrador proporciona un nivel alto de seguridad, adecuado para proteger la transferencia de información entre los PCs de nivel Brigada o superior.

Figura 34: Cifrador IP táctico EP430T. (Fuente: EPICOM)

- **Características**

Este cifrador está acreditado por el CCN para proteger todo tipo de información clasificada[11] y permite el cifrado de comunicaciones IP de hasta 200Mbps. Además, admite la programación de diferentes modos según el dominio de clasificación (Nacional u OTAN). Esto permitiría el empleo de esta arquitectura tanto a nivel de operaciones en territorio nacional como en misiones OTAN.

Este cifrador sólo admite conexión a través de fibra óptica. Por tanto, es necesario un conversor de cable UTP a fibra óptica, tanto para la entrada, como para la salida del cifrador, con vistas a utilizarlo en el sistema de radioenlace IP.

Figura 35: Trasceiver fibra óptica-UTP. (Fuente: https://articulo.mercadolibre.com.co)

La Figura 35 muestra el conversor utilizado en la entrada y salida del cifrador para el paso de cable UTP en fibra óptica y viceversa.

- **Funcionamiento**

Su funcionamiento consiste en cifrar vía IP todos los datos que se pretenden transmitir hacia el otro PC con el fin de que, si el mensaje es interceptado, sea imposible descifrar su contenido. Este dispositivo se coloca entre el switch y la antena del radioenlace, de forma que, todo lo que se quiere transmitir, es cifrado antes de la salida al radioenlace. Además, la información que le llega del otro PC se descifra antes de llegar a los dispositivos destinatarios.

La arquitectura del sistema con el cifrador instalado se muestra en la Figura 36.

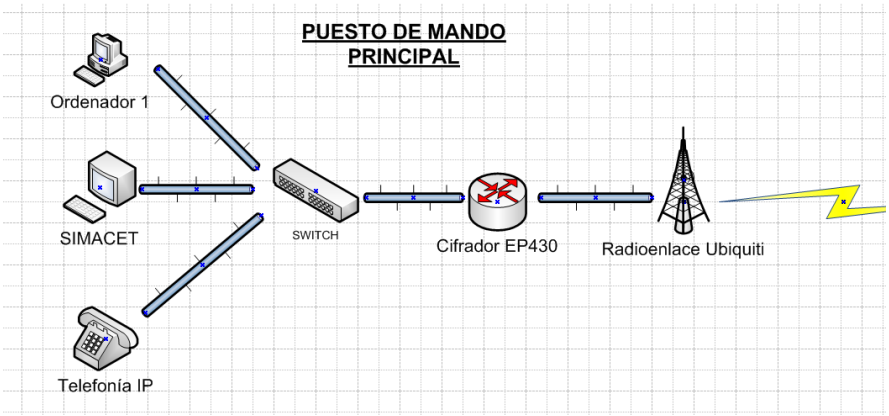


Figura 36: Arquitectura de red final de un PC. (Fuente: Elaboración propia)

El cifrador está colocado entre el switch y la antena. Hay que remarcar que la arquitectura de red del otro puesto de mando al que se transmite la información es simétrica.

A la hora de la configuración interna del cifrador, hay que indicarle por un lado las direcciones IP de los dispositivos (LAN) y por el otro la del propio radioenlace (WAN). También hay que predeterminar en ambos cifradores la clave que estos van a utilizar ya que, si no están sincronizados, será imposible el intercambio de información.

La información sale de una de las redes virtuales con una dirección IP hacía el cifrador, posteriormente se cifra el contenido y lo envía a la antena, la cual transmite dicha información encriptada al otro puesto de mando. En el segundo puesto de mando, una vez la antena recibe la información, la manda vía IP al cifrador. Este, que conoce la clave con la que fue encriptado el archivo, desencripta la información. Por último, el cifrador envía la información en claro al dispositivo final.

El método de cifrado, así como una configuración más detallada, no pueden hacerse públicas debido a que es material secreto del Ejército de Tierra.

- **Manipulación**

Este cifrador es material crítico por lo que su instalación sólo puede realizarse por personal que esté acreditado para ello. Además, es necesario que haya un constante control físico del dispositivo para evitar que nadie pueda manipularlo. Por ello se colocará dentro de un rack protegido.

Por último, en caso de que el personal no autorizado pueda hacerse con el cifrador, habría que presionar el botón de borrado de emergencia. Esto hará que se borren todas las claves de cifrado prestablecidas y así no permitir al enemigo hacerse con ellas para descifrar la posible información cifrada.

5.3. Seguridad física del equipo

Por último, se tratará el tema de la seguridad física referente a los dispositivos que conforman el radioenlace. Es muy importante que se controle el acceso físico a los cifradores y a las antenas ya que desde ellos se podría cambiar la configuración de la red de una forma sencilla. Cabe destacar que es muy complicado que un intruso entre en el perímetro de seguridad que tiene establecido cada PC.

El cifrador se colocará dentro del área de explotación del PC ya que va a haber más seguridad frente a intrusos y contra amenazas ambientales. Dentro del PC se instalará en el interior de un rack junto con el switch con un candado del que sólo dispondrá la llave el administrador de la estación de radioenlace.

Por otro lado, la antena, se colocará en el área herciana. Esta zona suele estar apartada del resto por lo que habría que destinar allí mínimo una persona que se encargue de su vigilancia. La antena se coloca en el mástil de un vehículo y desde su interior se podrá operar toda la configuración propia de la antena anteriormente descrita.

Figura 37: Vehículo Vamtac desde el que se opera el radioenlace. (Fuente: Elaboración propia)

La Figura 37 muestra el vehículo que se colocará en el área herciana. La flecha 1 señala la antena. Esta se coloca en lo alto del mástil y se conecta mediante un cable UTP al interior del vehículo. La flecha 2 señala el interior del vehículo desde el cual se opera la configuración de la antena a través de un ordenador portátil. Por último, desde esta estación se llevará un cable de fibra óptica hacia el interior de la zona de explotación del PC.

6. Conclusiones

En este capítulo se resumen los resultados obtenidos de los estudios realizados en este trabajo: Análisis y diseño del sistema y seguridad de los radioenlaces. Además, se mencionarán una serie de líneas de trabajo futuras que no han podido realizarse.

6.1. Conclusiones del análisis y diseño del sistema

Una vez finalizados los estudios previos a la elección de antena se puede afirmar que las antenas de las que dispone la unidad y las que utiliza actualmente el Ejército de Tierra en misiones internacionales cumplen los requisitos teóricos para la realización del radioenlace IP entre los dos PCs.

Una vez determinado el tipo de radioenlace óptimo, se procedió a la simulación mediante programas de software libre cómo Radio Mobile y simuladores propios de la compañía Ubiquiti, llegando a la conclusión de que dichas antenas permiten una calidad de enlace entre los dos PCs aceptable para media y larga distancia.

Posteriormente, se realizó una prueba de campo a partir de los datos de la simulación de medio alcance. Los resultados obtenidos en esta prueba han confirmado la capacidad y fiabilidad del tipo de radioenlaces IP propuestos en este trabajo.

En resumen, en estos apartados se ha llegado a la conclusión de que dichas antenas son más que fiables para una correcta transferencia de información entre PCs.

6.2. Conclusiones de la seguridad de los radioenlaces

Tras el estudio realizado anteriormente, en este capítulo se ha conseguido fortalecer la seguridad en los radioenlaces propuestos. Primeramente, se procedió a la configuración interna de la antena para hacer la red menos vulnerable a posibles ataques. Seguidamente se llegó a la conclusión de que es necesario el uso de un cifrador certificado para la transferencia de información sensible. Por último, después de estudiar la seguridad física del equipo, se puede afirmar que es necesario que haya personal destinado exclusivamente a la custodia de los dispositivos que componen la arquitectura final del radioenlace IP.

6.3. Líneas futuras

Durante la realización de este trabajo y las prácticas en la unidad, han ido surgiendo nuevas ideas y posibilidades que no han podido ser realizadas debido a falta de tiempo o por diversos motivos logísticos de la unidad.

A continuación, se detallan algunos de esos futuros trabajos:

- La distancia de la prueba de campo realizada fue de media distancia (5km). Sería necesario realizar otra prueba para distancias mayores y valorar los resultados.
- La climatología en la prueba de campo era muy favorable. Sería conveniente realizar otra prueba con meteorología adversa, es decir, con fuertes lluvias y viento para comprobar la estabilidad del enlace.
- Por último, no se pudo realizar ninguna prueba de ataque al sistema de radioenlace. A nivel teórico sería prácticamente imposible que un intruso accediese a la información transferida entre PCs. Aun así, sería recomendable realizar una serie de pruebas con el fin de atacar el sistema. Las posibles pruebas serían: Ataque contra la estabilidad del enlace, robo de la información y para finalizar intentar descifrar el contenido de la información.

Referencias

[1] MADOC, “PD4-502 MANDO DE ADIESTRAMIENTO Y DOCTRINA DEROGA: OR4-503, 2016. Empleo de la Unidad de Transmisiones de la Brigada.”

[2] R. L. Freeman, Radio system design for Telecommunications, John Wiley and Sons, Inc, 2007 .

[3] Francisco Ramos, “Perdida en obstáculos,” 2011. [Online]. Available: http://www.radioenlaces.es/articulos/perdidas-en-obstaculos/.

[4] WNI. México, “Tipos de antena y funcionamiento.” [Online]. Available: https://www.wni.mx/index.php?option=com_content&view=article&id=62:antenassoporte&catid=31:general&Itemid=79.

[5] Unión Internacional de Telecomunicaciones, 2017, “Características De La Precipitación Para Establecer Modelos De Propagación,” pp. 1–4.

[6] Software. Libre, “Radiomobile.” [Online]. Available: https://www.ve2dbe.com/.

[7] Ubiquiti, “AirLink.” [Online]. Available: https://link.ui.com/#.

[8] CCN, “Requisitos STIC (CCN-STIC 301),” 2018.

[9] Telecommunications: Glossary of Telecommunication Terms, Government Institutes, 1997.

[10] CCN, “Guía de Seguridad de las TIC Seguridad en Redes Inalámbricas,” 2017.

[11] CCN, “Guía de Seguridad de las TIC Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación,” 2019.

[12] I. D. E. S. Del, “ORIENTACIONES PARA LA INSTRUCCIÓN DE SEGURIDAD DEL PERSONAL PARA ACCESO A INFORMACIÓN CLASIFICADA,” pp. 1–97.

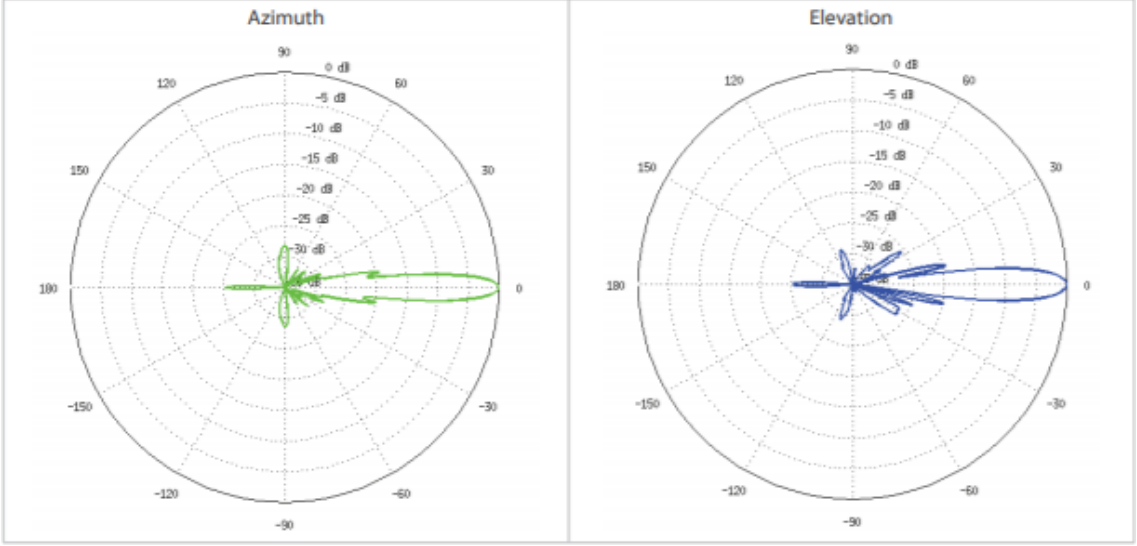
ANEXOS

ANEXO A: Especificaciones técnicas de la antena Ubiquiti AG-HP-5G27.

AG-HP-5G27	
Dimensions (Mount Included)	620 x 460 x 360 mm (24.41 x 18.11 x 14.17")
Weight (Mount Included)	2585 g (5.699 lb)
Wind Survivability	200 km/h (125 mph)
Wind Loading	102 N @ 200 km/h (23 lbf @ 125 mph)
Operating Frequency	5725 - 5850 MHz
Max. VSWR	1.5:1
Gain	27 dBi

AG-HP-5G27 Output Power: 25 dBm							
TX Power Specifications				**RX Power Specifications**			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
11a	1 - 24 Mbps	25 dBm	± 2 dB	11a	1 - 24 Mbps	-97 dBm min.	± 2 dB
	36 Mbps	24 dBm	± 2 dB		36 Mbps	-90 dBm	± 2 dB
	48 Mbps	22 dBm	± 2 dB		48 Mbps	-86 dBm	± 2 dB
	54 Mbps	21 dBm	± 2 dB		54 Mbps	-84 dBm	± 2 dB
11n / airMAX	MCS0	25 dBm	± 2 dB	11n / airMAX	MCS0	-97 dBm	± 2 dB
	MCS1	25 dBm	± 2 dB		MCS1	-96 dBm	± 2 dB
	MCS2	25 dBm	± 2 dB		MCS2	-93 dBm	± 2 dB
	MCS3	24 dBm	± 2 dB		MCS3	-91 dBm	± 2 dB
	MCS4	23 dBm	± 2 dB		MCS4	-87 dBm	± 2 dB
	MCS5	22 dBm	± 2 dB		MCS5	-84 dBm	± 2 dB
	MCS6	21 dBm	± 2 dB		MCS6	-78 dBm	± 2 dB
	MCS7	19 dBm	± 2 dB		MCS7	-75 dBm	± 2 dB

Antenna Polar Plots



ANEXO B: Especificaciones técnicas del transmisor Ubiquiti Rocket M5.

rocket M5

M5 Physical / Electrical / Environmental Information	
Dimensions	160 x 80 x 30 mm (6.30 x 3.15 x 1.18")
Weight	500 g (1.1 lb)
Enclosure Characteristics	Outdoor UV Stabilized Plastic
Processor	MIPS 74Kc
Memory	128 MB SDRAM, 8 MB Flash
Networking Interface	(1) 10/100 Mbps
RF Connections	(2) RP-SMA (Waterproof)
LEDs	Power, Ethernet, (4) Signal Strength
Max. Power Consumption	8W
Power Supply	24V, 1A PoE Adapter
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)
ESD/EMP Protection	± 24KV Air / Contact
Operating Temperature	-30 to 75° C (-22 to 167° F)
Operating Humidity	5 to 95% Noncondensing
Shock and Vibration	ETSI300-019-1.4

M5 Software Information	
Modes	Access Point, Station
Services	Web Server, SNMP, SSH Server, Telnet , Ping Watchdog, DHCP, NAT, Bridging, Routing
Utilities	Antenna Alignment Tool, Discovery Utility, Site Survey, Ping, Traceroute, Speed Test
Distance Adjustment	Dynamic Ack and Ackless Mode
Power Adjustment	Software Adjustable UI or CLI
Security	WPA2 AES Only
QoS	Supports Packet Level Classification WMM and User Customer Level: High/Medium/Low
Statistical Reporting	Up Time, Packet Errors, Data Rates, Wireless Distance, Ethernet Link Rate
Other	Remote Reset Support, Software Enabled/Disabled, VLAN Support, 64QAM, 5/8/10/20/30/40 MHz Channel Width Support
Ubiquiti Specific Features	airMAX Mode, Traffic Shaping with Burst Support, Discovery Protocol, Frequency Band Offset, Ackless Mode

M5 Compliance	
Wireless Approvals	FCC, IC, CE
RoHS Compliance	Yes

M5 Operating Frequency							
Operating Frequency			Worldwide: 5170 - 5875 MHz USA: 5725 - 5850 MHz*				
Output Power			27 dBm				
TX Power Specifications				**RX Power Specifications**			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
802.11a	6 - 24 Mbps	27 dBm	± 2 dB	802.11a	6 - 24 Mbps	-94 dBm Min.	± 2 dB
	36 Mbps	25 dBm	± 2 dB		36 Mbps	-80 dBm	± 2 dB
	48 Mbps	23 dBm	± 2 dB		48 Mbps	-77 dBm	± 2 dB
	54 Mbps	22 dBm	± 2 dB		54 Mbps	-75 dBm	± 2 dB
802.11n/airMAX	MCS0	27 dBm	± 2 dB	802.11n/airMAX	MCS0	-96 dBm	± 2 dB
	MCS1	27 dBm	± 2 dB		MCS1	-95 dBm	± 2 dB
	MCS2	27 dBm	± 2 dB		MCS2	-92 dBm	± 2 dB
	MCS3	27 dBm	± 2 dB		MCS3	-90 dBm	± 2 dB
	MCS4	26 dBm	± 2 dB		MCS4	-86 dBm	± 2 dB
	MCS5	24 dBm	± 2 dB		MCS5	-83 dBm	± 2 dB
	MCS6	22 dBm	± 2 dB		MCS6	-77 dBm	± 2 dB
	MCS7	21 dBm	± 2 dB		MCS7	-74 dBm	± 2 dB
	MCS8	27 dBm	± 2 dB		MCS8	-95 dBm	± 2 dB
	MCS9	27 dBm	± 2 dB		MCS9	-93 dBm	± 2 dB
	MCS10	27 dBm	± 2 dB		MCS10	-90 dBm	± 2 dB
	MCS11	27 dBm	± 2 dB		MCS11	-87 dBm	± 2 dB
	MCS12	26 dBm	± 2 dB		MCS12	-84 dBm	± 2 dB
	MCS13	24 dBm	± 2 dB		MCS13	-79 dBm	± 2 dB
	MCS14	22 dBm	± 2 dB		MCS14	-78 dBm	± 2 dB
	MCS15	21 dBm	± 2 dB		MCS15	-75 dBm	± 2 dB

* US units with FCC ID: SWX-RM5 are allowed 5250 - 5850 MHz.

ANEXO C: Especificaciones técnicas de la antena RD-5G34

Model	Frequency	Gain[1]	Radome[2]
RD-5G34	4.9 - 5.8 GHz	30 - 34 dBi	RAD-RD3

The RD-5G34 offers up to 34 dBi of gain in a 1050-mm diameter size.

ANEXO D: Simulaciones realizadas con la aplicación oficial de Ubiquiti

❖ **Simulación de largo alcance**

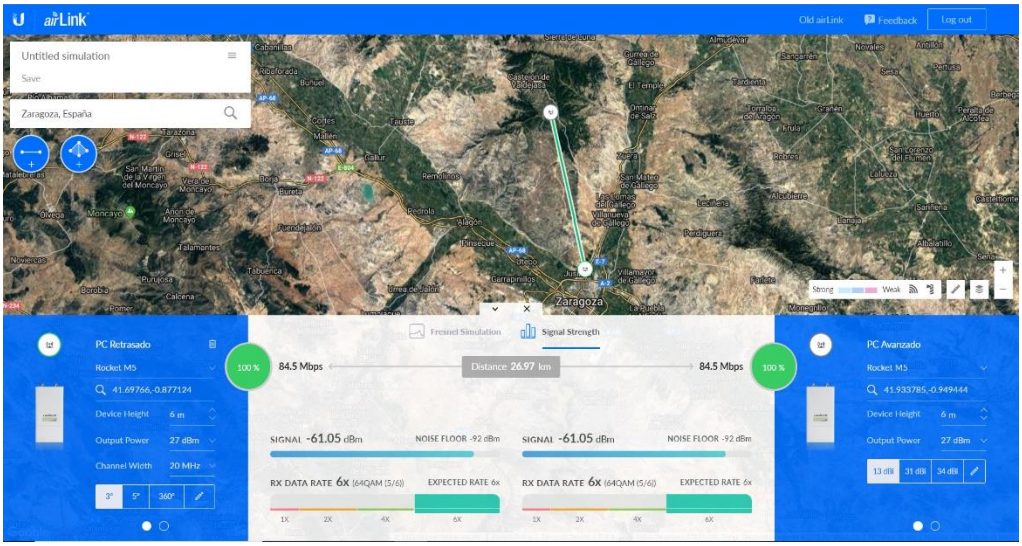


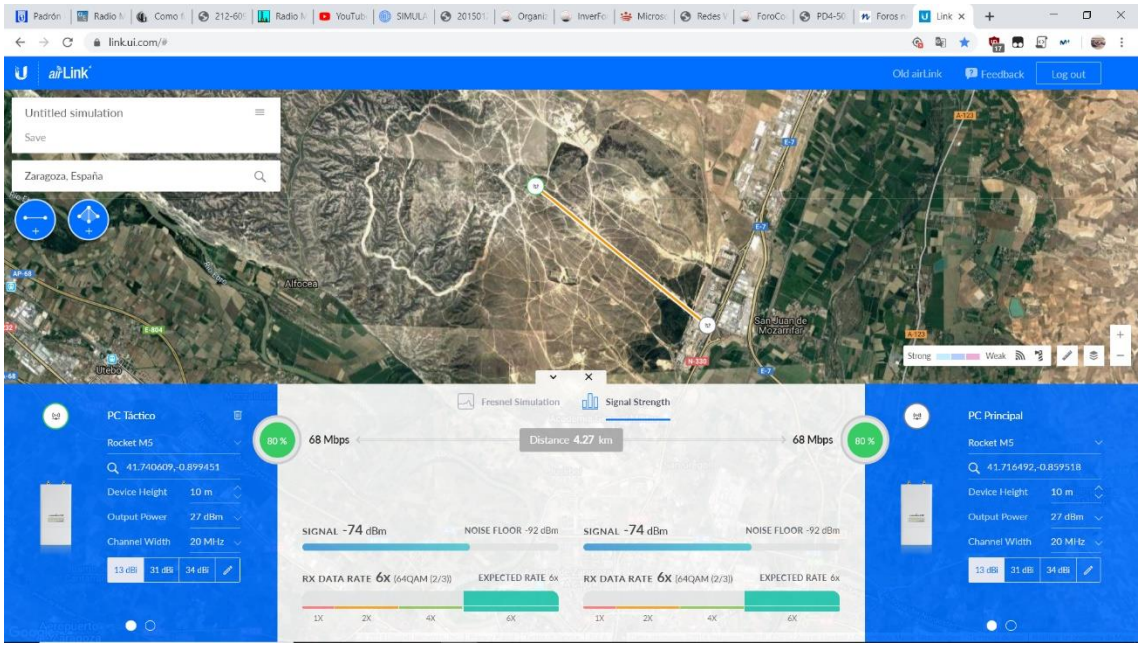
Figura 38: Simulación antena Ubiquiti Rocket M5 (Fuente: Elaboración propia)

Para la antena Rocket M5 hemos realizado las simulaciones a través de la página web oficial de la empresa Ubiquiti, concretamente con la aplicación AirLink. En dicha página simplemente se selecciona la antena con la que se va a trabajar, en este caso la Ubiquiti Rocket M5 y se colocan los dos PCs en las coordenadas marcadas, la altura a la que se colocan las antenas y la potencia (En este caso la máxima). El mismo programa ya recoge todos los parámetros de dicha antena y nos indica si habrá enlace o no según el color:

- Verde: Enlace totalmente favorable.
- Naranja: Enlace establecido, pero no al 100% de sus capacidades.
- Rojo: No hay posibilidad de establecer enlace correctamente.

En este caso el enlace se podrá realizar sin ningún problema ya que el nivel de señal es -61,05 dBm.

- **Simulación de medio alcance**



El nivel de señal es de -74 dBm por lo que en enlace sería satisfactorio, aunque no al 100% de sus capacidades.

ANEXO E: Grados de protección de la información

A continuación, se describen los grados de protección de la información de mayor a menor relevancia [12]:

- SECRETO: Se concederá a la información que necesite el grado más alto de protección. Además, la revelación no autorizada de esta pueda dar lugar a una amenaza extremadamente grave o comprometer los intereses fundamentales del estado referente a materia de defensa nacional, orden constitucional o paz exterior.

- RESERVADO: Se concederá a la información que necesite un grado de protección elevado. Además, la revelación no autorizada de esta pueda perjudicar gravemente a los intereses del estado.

- CONFIDENCIAL: Se concederá a la información cuyo conocimiento por personas no autorizadas afecte a la propia seguridad estatal o amenace sus intereses.

- DIFUSIÓN LIMITADA: Se concederá a la información que sólo podrá ser manejada por el personal instruido en materia de información clasificada. La revelación no autorizada de esta información podría ser contraria a los intereses de España.